

Claims

What is claimed is:

1. A system enabling an application to produce a response to an authentication challenge, comprising:
an authentication manager adapted to receive a first data associated with the communication challenge and to process the first data into a second data, the authentication manager further operable to communicate the second data to at least one authentication module, the second data related to the first data and the authentication challenge; and
at least one authentication module adapted to receive the second data from the authentication manager and to produce a third data related to responding to the authentication challenge.
2. The system of claim 1, comprising a cache adapted to store one or more third data related to responding to the authentication challenge.
3. The system of claim 1, wherein the authentication manager is further adapted to receive a set of first data associated with a multipart authentication challenge, to process the set of first data into a set of second data, and to communicate the set of second data to at least one authentication module, the set of second data related to the set of first data and the multipart authentication challenge.
4. The system of claim 3, wherein the at least one authentication module is further adapted to receive a set of second data from the authentication manager and to produce a set of third data related to responding to the multipart authentication challenge.
5. The system of claim 4, wherein the cache is further adapted to store a set of third data related to responding to the multipart authentication challenge.

6. The system of claim 2, wherein:

the authentication manager is further adapted to accept a pre-authentication challenge test message associated with an anticipated communication challenge, to process the test message into a fourth data, and to communicate the fourth data to at least one authentication module, the fourth data related to the pre-authentication challenge test message;

at least one authentication module is further adapted to receive the fourth data from the authentication manager and to produce a fifth data related to responding to the pre-authentication challenge test message; and

the cache is further adapted to store one or more fifth data related to responding to the pre-authentication challenge test message, the cache operable to selectively provide the fifth data upon request by the authentication manager.

7. The system of claim 6, wherein the authentication modules are further adapted to pass a sixth data to one or more services, the services employed to facilitate producing the third data.

8. The system of claim 1, comprising:

a class factory, the class factory operable to selectively instantiate one or more authentication objects based, at least in part, on the first data, and

the class factory operable to make the one or more instantiated authentication objects callable by the authentication manager.

9. The system of claim 8, comprising:

a data store operable to hold information associated with selectively instantiating the one or more authentication objects, the data store further operable to hold information associated with making the one or more instantiated authentication objects callable by the authentication manager.

10. The system of claim 9, comprising:

a registrar adapted to register an authentication object with the class factory.

11. The system of claim 10, wherein the registrar is further adapted to register an authentication object with the data store.
12. The system of claim 11, wherein the application does not have to be recoded or recompiled to employ the newly registered authentication object.
13. The system of claim 1, wherein one or more authentication objects are operable to generate third data associated with responding to an authentication challenge associated with at least one of, a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.
14. The system of claim 1, wherein the authentication manager and the one or more authentication objects are distributed to one or more distributed processors.
15. The system of claim 11, wherein the class factory, the data store and the registrar are distributed to one or more distributed processors.
16. A method for enabling an application to produce a response to an authentication challenge, comprising:
 - accepting an authentication challenge;
 - passing a first data associated with the authentication challenge to an authentication manager, where the authentication manager is operable to pass data to one or more authentication modules;
 - passing a second data associated with the authentication challenge to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager; and
 - producing one or more responses to the authentication challenge.

17. The system of claim 16, comprising:
caching one or more responses to the authentication challenge; and
retrieving a response from the cached responses.
18. The method of claim 16, wherein the authentication challenge is generated by at least one of a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.
19. The method of claim 16, wherein one or more authentication modules can be created and registered after the receipt of one or more authentication challenges.
20. A computer readable medium, comprising:
computer executable instructions operable to perform the method of claim 16.
21. The computer readable medium of claim 20, further comprising computer executable instructions operable to perform the method of claim 19.

22. A method for enabling an application to produce a response to an authentication challenge, comprising:

generating a pre-authentication challenge test message;

passing a first data associated with the pre-authentication challenge test message to an authentication manager, where the authentication manager is operable to pass data to one or more authentication modules;

passing a second data associated with the pre-authentication challenge test message to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager;

producing one or more responses to the pre-authentication challenge test message;

and

caching the one or more responses to the pre-authentication challenge test message.

23. The method of claim 22, wherein the pre-authentication challenge test message is related to an authentication challenge generated by at least one of a Kerberos authentication system, a Digest authentication system, a Basic authentication system, an NTLM authentication system and a certificate based authentication system.

24. The method of claim 22, wherein one or more authentication modules can be created and registered after the generation of one or more pre-authentication challenge test messages.

25. The method of claim 22, wherein the application does not have to be recoded or recompiled to employ the newly registered authentication modules.

26. A computer readable medium having computer executable instructions operable to perform a method comprising:
- generating a pre-authentication challenge test message;
 - passing a first data associated with the pre-authentication challenge test message to an authentication manager, where the authentication manager is operable to pass data to one or more authentication modules;
 - passing a second data associated with the pre-authentication challenge test message to one or more authentication modules, where the authentication modules are registered with the authentication manager, and where the authentication modules are operatively connected to the authentication manager;
 - producing one or more responses to the pre-authentication challenge test message;
- and
- caching the one or more responses to the pre-authentication challenge test message.
27. A data packet adapted to be transmitted between two or more computer processes, the data packet containing information related to selecting an authentication object to process data associated with an authentication challenge.
28. A data packet adapted to be transmitted between two or more computer processes, the data packet containing information related to registering an authentication object with a class factory and a data store, wherein registering the authentication object facilitates an authentication manager employing the authentication object to produce a response to an authentication challenge.
29. A data packet adapted to be transmitted between two or more computer processes, the data packet containing a response to an authentication challenge, where the response was generated by an authentication module adapted to receive data from an authentication manager and to send the response to the authentication manager.

30. A system enabling an application to respond to a challenge to a request to access a resource addressable by a URI, comprising:

receiving means for receiving a challenge, the receiving means separate from the application;

distributing means for distributing the challenge to one or more producing means, the distributing means being separate from the application;

producing means for producing a response to the challenge; the producing means being separate from the application; and

storing means for storing a response to the challenge.